The Dissertation Committee for Rohit Ghosh certifies that this is the approved version of the following dissertation:

Incompleteness of the Giulietti-Ughi arc for Large Primes

Committee:

_____

José Felipe Voloch, Supervisor

_____

James Hirschfeld

_____

Fernando Rodriguez-Villegas

_____

Sean Keel

_____

Jeffrey Vaaler

Incompleteness of the Giulietti-Ughi arc for Large Primes

by

Rohit Ghosh, B.Sc; M.Sc

Dissertation

Presented to the Faculty of the Graduate School of

the University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Doctor of Philosophy

The University of Texas at Austin

December 2007

Acknowledgments

My appreciation and thanks is owed to many people. First, I would like to thank my adviser and friend Felipe Voloch for his insight, patience and encouragement. I am also greatly indebted to my family and friends for their support and understanding. Finally, a special note of thanks is due to my entire dissertation committee.

Incompleteness of the Giulietti-Ughi arc for Large Primes

Publication No. _____

Rohit Ghosh, Ph.D.

The University of Texas at Austin, 2007

Supervisor: José Felipe Voloch

In this dissertation we show that the Giulietti-Ughi arc is not complete for large primes. This arc is complete for primes which are congruent to three modulo four and less than thirty one. The cardinality of this arc has the same order as the Lunelli-Sce bound. We use two powerful theorems, one on the classifications of Galois groups of quintic polynomials and the other, the Čebotarev density theorem for function fields to show that there exist points on a certain curve which are not covered by the arc. We then outline a technique which could be used to extend the arc to a complete arc.

Contents

Chapter 1

Introduction

1.1 Basic Concepts

This dissertation deals with properties of certain structures defined on a projective plane over a finite field. We begin by defining a projective plane of order m.

Definition 1. *A projective plane of order m is a set of m^2+m+1 elements called points , together with m^2+m+1 distinguished sets of points, called lines, as well as a relation I , called incidence, between lines and points subject to the following conditions:*

1. *Every pair of distinct lines is incident with a unique point.*
2. *Every pair of distinct points is incident with a unique line*
3. *There exist four points such that no three of them are incident with a single line.*

Note that the axioms above are self-dual. Hence the dual of a projective plane is a projective plane. We will see that there exists a projective plane of order m for every integer m of the form $m = p^n$, where p is a prime. It is known that there is no plane for $m = 6, 10$ but it is not known whether a plane exists for $m = 12$. No plane has yet been found where m is not a prime power.

Conjecture (Prime Power Conjecture)**.** *The order of every finite projective plane is a prime power.*

We will now define a projective plane over a finite field $\mathbb{F}_q$.

Definition 2. *Let V be a vector space of dimension three over $\mathbb{F}_q$. The projective plane $PG(2,q)$ is the geometry whose points and lines are subspaces of V whose dimensions are one and two respectively and the incidence relation is given by containment.*

Since the points and lines of $PG(2,q)$ satisfy the axioms of definition 1 there exists for every prime power q a projective plane of order q. We also define $AG(2,q)$ to be $PG(2,q)\backslash\{$ a line$\}$. We can represent $PG(2,q)$ by the union of the sets

$$\{(l,m,1)\,|\,l,m\in\mathbb{F}_q\}\cup\{(l,1,n)\,|\,l,n\in\mathbb{F}_q\}\cup\{(1,m,n)\,|\,m,n\in\mathbb{F}_q\}$$

and in this dissertation when we refer to $AG(2,q)$ we will be referring to the affine plane obtained by removing the line $n=0$ i.e. the first set in the union. In most cases when we refer to a point in $AG(2,q)$ we drop the last coordinate as we take $n=1$ and write the point simply as (l,m). We will study subsets of the projective plane called arcs and complete arcs.

Definition 3. *An arc is a set of points in a projective plane such that no three points are collinear. An arc which is maximal under inclusion is called a complete arc.*

Another way of characterizing complete arcs is that every point in $PG(2,q)$ lies on a line (secant) formed by joining two points on the arc. We must caution the reader that an arc is a purely combinatorial object as opposed to a curve which is algebraic in nature.

1.2 Arcs

After introducing the concept of the arc in the 1950's, Segre asked questions about the size of complete arcs. For q odd, the maximum size of a complete arc is $q+1$ and for q even it is $q+2$. A celebrated theorem of Segre's states that in the odd case the maximum is attained if and only if the arc is a conic; however in the even case the characterization is not yet complete ([3]). Bounds for the size of the second

largest complete arc have also been obtained([9, 10, 13, 15, 14]). In this case some of the particularly interesting results have been obtained by using the Stöhr-Voloch bound for estimating points on algebraic curves over finite fields ([14]).

Constructing complete arcs of minimal size is essentially a mini-max problem as we want to choose a set of points of small cardinality such that every point in $PG(2,q)$ lies on at least one secant. Let n_q denote the size of the smallest complete arc in a projective plane of order q.

Theorem 1 (Lunelli-Sce)**.** *The cardinality of the smallest complete arc is at least* $\sqrt{2q}$ *i.e.* $n_q \geq \sqrt{2q}$.

Proof. We know that $PG(2,q)$ contains q^2+q+1 points and that every line contains $q+1$ points. Hence a complete arc must have at least $\frac{q^2+q+1}{q+1} \geq q$ secants. Let n be the cardinality of an arc. The number of secants an arc of cardinality n possesses is $\frac{n(n-1)}{2}$ and this number must be at least q for the arc to be complete. The bound now follows from the inequality $\frac{n(n-1)}{2} \geq q$. □

Blokhuis and Ball improved the Lunelli-Sce bound to $\sqrt{3q}$ when q is a prime or the square of a prime respectively ([1, 2]). Fisher conjectured that the average size of a complete arc is $\sqrt{3q \log q}$ ([6]). One of the most important results in this field is due to Kim and Vu who prove that $n_q \leq \sqrt{q} \log^c q$ where c is a universal constant ([11]). They use a probabilistic method known as Rödl nibble to show the existence of an arc satisfying the above inequality without explicitly constructing one. This together with the Lunelli-Sce bound determines n_q up to a polylogarithmic factor.

Giulietti and Ughi construct a small arc in $PG(2,q)$ where $q = p^2$ and $p \equiv 3 \bmod 4$ of size $4(\sqrt{q}-1)$ ([8]). This arc is known to be complete for primes $p \leq 31$. The cardinality of this arc is close to the Lunelli-Sce bound. The natural question one could ask is if this arc is complete for larger primes and if not would it be possible to construct a complete arc of cardinality close to the Lunelli-Sce bound by adding points to the arc.

1.3 The Giulietti-Ughi arc

In [8] Giulietti and Ughi construct a small arc in $PG(2,q)$ where $q = p^2$ and $p \equiv 3 \bmod 4$. Since $p \equiv 3 \bmod 4$ we have that $\mathbb{F}_q \cong \mathbb{F}_p(i)$, with $i^2 = -1$. Throughout this dissertation we shall assume that our primes p satisfy $p \equiv 3 \bmod 4$ and $q = p^2$. The arc is constructed by choosing points on the conics $xy = 1$ and $xy = i$ in $PG(2,q)$. Let

$$\begin{aligned} K_1 &= \{(\alpha, \frac{1}{\alpha}) \,|\, \alpha \in \mathbb{F}_p^*\} \\ K_2 &= \{(\beta, \frac{i}{\beta}) \,|\, \beta \in \mathbb{F}_p^*\} \\ K_3 &= \{(i\gamma, \frac{1}{\gamma}) \,|\, \gamma \in \mathbb{F}_p^*\} \\ K_4 &= \{(i\delta, \frac{-i}{\delta}) \,|\, \delta \in \mathbb{F}_p^*\}. \end{aligned}$$

Then $K = K_1 \cup K_2 \cup K_3 \cup K_4$ is a arc of cardinality $4(\sqrt{q} - 1)$ and is known to be complete for primes $p \leq 31$. In this dissertation we prove that for all sufficiently large primes the arc K will not be complete.

1.4 Results

In this dissertation we prove the following theorems.

Theorem 2. *For all sufficiently large primes the Giulietti-Ughi arc is not complete.*

We prove this theorem using results from Galois theory and the Čebotarev density theorem for function fields. A natural question one could ask is whether this construction can be extended further. In other words, is it possible to add sets of points lying on conics to the original arc and obtain a complete arc for larger primes. In this dissertation we also demonstrate a technique which could potentially be used to do precisely this.

Theorem 3. *For all sufficiently large primes the number of points lying on the curve given by* $\{[t^2 + it, t^2 + t + i, 1] \,|\, t \in \mathbb{F}_p\}$ *which may be added to the Giulietti-Ughi arc to construct a larger arc is* $(\frac{1}{2})^6(\frac{11}{30})^4(\frac{1}{3})^4 p + O(\sqrt{p})$.

Chapter 2

Background

2.1 Computational Tools

In this dissertation most computations will involve using the following two theorems.

Theorem 4. *Let $f(t) \in \mathbb{Q}(t)$. Assume that $f(t) \neq cg(t)^2$ where $c \in \mathbb{Q}$ and $g(t) \in \mathbb{Q}(t)$ i.e. $f(t)$ is not a constant times a square. Then for all sufficiently large primes we have that $f(t) \in \mathbb{F}_p(t)$ and is not a constant times a square.*

Proof. Let $f(t) = cf_1(t)^{n_1} \dots f_r(t)^{n_r}$ where $f_i(t)$ are distinct irreducible polynomials, $c \in \mathbb{Q}$ and $n_i \in \mathbb{Z}$. By hypothesis at least one n_i is odd. Assume without loss of generality that n_1 is odd. We choose primes sufficiently large satisfying the following conditions:
i) None of the factors coincide or become zero when $f(t)$ is reduced $\bmod p$.
ii) The primes p do not divide the discriminant of f_1 and f_1 is not congruent to a constant when reduced $\bmod p$.
iii) The primes p do not divide Resultant(f_1,f_i) for $i \in \{1, 2, \cdots, r\}$ and $i \neq 1$.
For primes satisfying these conditions f_1 has no repeated factors nor has any factor common with $f_2, \cdots, f_r$. Hence for all sufficiently large primes $f(t) \in \mathbb{F}_p(t)$ and is not a constant times a square. □

Theorem 5. *There are only finitely many primes p for which an absolutely irreducible multivariate polynomial g over $\mathbb{Q}$ is not absolutely irreducible* $\bmod p$.

Proof. See [12] Lemma 3 on page 173. □

All the programs in this dissertation were implemented in $MAGMA$ except absolute irreducibility was checked using $MAPLE$. In a few cases our polynomials will belong to $\mathbb{Q}(t)[b]$ but to check absolute irreducibility we want our polynomials to belong to $\mathbb{Q}[t, b]$. We multiply these polynomials by a suitable element of $\mathbb{Q}[t]$ to clear denominators. The polynomials now belongs to $\mathbb{Q}[t, b]$ and we can test for absolute 0. Since we are ultimately interested in 0 over $\mathbb{Q}(t)$ and $\mathbb{F}_p(t)$ this is equivalent to multiplying the polynomials by a constant.

2.2 Čebotarev Density Theorem

Let $f(b, t)$ be a bivariate polynomial defined over $\mathbb{F}_p$ of degree n in b . For $t_0 \in \mathbb{F}_p$ such that $\deg(f(b, t_0)) = n$, we factor $f(b, t_0)$ over $\mathbb{F}_p$ as

$$f = f_1 f_2 \dots f_r.$$

Let n_i be the degree of f_i in the equation above. We permute the factors so that $n_i \leq n_j$ for $i < j$. To each $t_0 \in \mathbb{F}_p$ we associate the tuple $\tau = (n_1, \dots, n_r)$. Since $n_1 + \dots + n_r = n$ we view τ as a partition of n. We refer to τ as the factorization type of t_0.

We state the following version of the Čebotarev density theorem (see [7]).

Theorem 6. *Let $f(b, t) \in \mathbb{F}_p(t)[b]$ be an irreducible separable polynomial of degree n when considered as a univariate polynomial defined over $\mathbb{F}_p(t)$. Let F be the splitting field of f over $\mathbb{F}_p(t)$ and G be the corresponding Galois group considered as a subgroup of S_n. Let C_τ denote the set of elements of G with factorization type τ. If $\mathbb{F}_p$ is algebraically closed in F, then the number of elements t in the set $\{t \in \mathbb{F}_p : \deg(f(b, t)) = n\}$ which have the same factorization type τ is $\frac{|C_\tau|}{|G|}p + O(\sqrt{p})$.*

The theorem can also be applied to a reducible separable polynomial whose splitting field satisfies the hypothesis of the theorem.

2.3 Galois Groups of the Quintic

To apply the Čebotarev density theorem to the polynomials in this dissertation we will need to study the transitive subgroups of S_5. There are six possibilities for the Galois group of an irreducible quintic. The Galois groups and the relationships between them are described by figure 2.1.

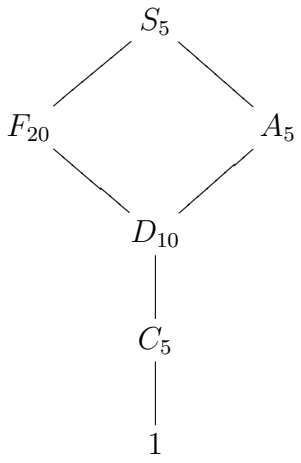

Figure 2.1: Galois Groups of the Quintic

If the square root of the discriminant of the polynomial does not belong to the base field then the only possible Galois Groups are S_5 and F_{20}. We use the following theorem (see [4]) to distinguish between the two groups.

Theorem 7 (Dummit)**.** *Let $\mathbb{F}$ be any field of characteristic different from two and five. Then an irreducible quintic $f(x) \in \mathbb{F}[x]$ is solvable by radicals if and only if its Galois group as a subgroup of S_5 is contained in the Frobenius Group of order 20 (F_{20}). The irreducible quintic $g(x) = x^5 + mx^3 + lx^2 + rx + s \in \mathbb{F}[x]$ is solvable by radicals if and only if the polynomial $h_{20}(x)$ (defined below) has a rational root. In this case the sextic polynomial $h_{20}(x)$ factors into the product of a linear polynomial and an irreducible quintic.*

$$
\begin{aligned}
h_{20}(x) = {} & x^6 + 8rx^5 + (2ml^2 - 6m^2r + 40r^2 - 50ls)x^4 \\
& (-2l^4 + 21ml^2 - 40m^2r^2 + 160r^3 - 15m^2ls - 400rs + 125ms^2)x^3 \\
& + (m^2l^4 - 6m^3l^2r - 8l^4r + 9m^4r^2 + 76ml^2r^2 - 136m^2r^3 \\
& + 400r^4 - 50ml^3s + 90m^2ls - 1400lr^2s + 625l^2s^2 + 500mrs^2)x^2 \\
& + (-2ml^6 + 19m^2l^4r - 51m^3q^2r + 3q^4r^2 + 32m^4r^3 + 76mq^2r^3 \\
& - 256m^2r^4 + 512r^5 - 31m^3l^3s - 58l^5s + 117m^4lrs + 105lm^3rs \\
& + 260m^2lr^2s - 2400lr^3 - 108m^5s^2 - 325m^2l^2s^2 + 525m^3rs^2 \\
& 2750l^2rs^2 - 500mr^2s^2 + 625lms^3 - 3125s^4)x \\
& + (l^8 - 13ml^6r + m^5l^2r^2 + 65m^2l^4r^2 - 4m^6r^3 - 128m^3l^2r^3 + 17l^4r^3 \\
& 48m^4r^4 - 16ml^2r^4 - 192m^2r^5 + 256r^6 - 4m^5l^3s - 12m^2l^5s \\
& 18m^6lrs + 12m^3l^3rs - 124l^5rs + 196m^4lr^2s + 590ml^3r^2s \\
& - 160m^2lr^3s - 1600lr^4s - 27m^7s^2 - 150m^4l^2s^2 - 125ml^4s^2 \\
& - 99m^5rs^2 - 725m^2l^2rs^2 + 1200m^3r^2s^2 + 3250l^2r^2s^2 \\
& - 2000mr^3s^2 - 1250mlrs^3 + 3125m^2s^4 - 9375rs^4).
\end{aligned}
$$

Chapter 3

Incompleteness of the Giulietti-Ughi arc

3.1 Condition for a point not to be covered

Throughout this chapter we will use the notations introduced in Chapter 1. A point in $PG(2,q)$ is said to be covered by the arc K if it lies on at least one of the secants of the arc. Otherwise, a point in $PG(2,q)$ is said to be a missing point. Let $P=(x+iw, y+iz)$ be a point in $AG(2,q)$ where x, w, y and z are elements of $\mathbb{F}_p$. The point P lies on a secant of the arc joining two distinct points in K_1 if and only if the equation

$$\begin{vmatrix} x+iw & y+iz & 1 \\ a & 1/a & 1 \\ b & 1/b & 1 \end{vmatrix} = 0$$

has a solution in $\mathbb{F}_p^* \times \mathbb{F}_p^*$ i.e. both a and b must belong to $\mathbb{F}_p^*$. Similarly P lies on a secant joining a point in K_1 to a point in K_2 if and only if

$$\begin{vmatrix} x+iw & y+iz & 1 \\ a & 1/a & 1 \\ b & i/b & 1 \end{vmatrix} = 0$$

has a solution in $\mathbb{F}_p^* \times \mathbb{F}_p^*$.

We list below the conditions P must satisfy in order to lie on a secant joining a point in K_i to a point in K_j in terms of polynomials $c_{ij}(a,b)$:

$$c_{11}(a,b) := ab \begin{vmatrix} x+iw & y+iz & 1 \\ a & 1/a & 1 \\ b & i/b & 1 \end{vmatrix} = 0 \text{ has a solution in } \mathbb{F}_p^* \times \mathbb{F}_p^*, \tag{3.1}$$

$$c_{22}(a,b) := ab \begin{vmatrix} x+iw & y+iz & 1 \\ a & i/a & 1 \\ b & i/b & 1 \end{vmatrix} = 0 \text{ has a solution in } \mathbb{F}_p^* \times \mathbb{F}_p^*, \tag{3.2}$$

$$c_{33}(a,b) := ab \begin{vmatrix} x+iw & y+iz & 1 \\ ia & 1/a & 1 \\ ib & 1/b & 1 \end{vmatrix} = 0 \text{ has a solution in } \mathbb{F}_p^* \times \mathbb{F}_p^*, \tag{3.3}$$

$$c_{44}(a,b) := ab \begin{vmatrix} x+iw & y+iz & 1 \\ ia & -i/a & 1 \\ ib & -i/b & 1 \end{vmatrix} = 0 \text{ has a solution in } \mathbb{F}_p^* \times \mathbb{F}_p^*, \tag{3.4}$$

$$c_{12}(a,b) := ab \begin{vmatrix} x+iw & y+iz & 1 \\ a & 1/a & 1 \\ b & i/b & 1 \end{vmatrix} = 0 \text{ has a solution in } \mathbb{F}_p^* \times \mathbb{F}_p^*, \tag{3.5}$$

$$c_{13}(a,b) := ab \begin{vmatrix} x+iw & y+iz & 1 \\ a & 1/a & 1 \\ ib & 1/b & 1 \end{vmatrix} = 0 \text{ has a solution in } \mathbb{F}_p^* \times \mathbb{F}_p^*, \tag{3.6}$$

$$c_{14}(a,b) := ab \begin{vmatrix} x+iw & y+iz & 1 \\ a & 1/a & 1 \\ ib & -i/b & 1 \end{vmatrix} = 0 \text{ has a solution in } \mathbb{F}_p^* \times \mathbb{F}_p^*, \tag{3.7}$$

$$c_{23}(a,b) := ab \begin{vmatrix} x+iw & y+iz & 1 \\ a & i/a & 1 \\ ib & 1/b & 1 \end{vmatrix} = 0 \text{ has a solution in } \mathbb{F}_p^* \times \mathbb{F}_p^*, \tag{3.8}$$

$$c_{24}(a,b) := ab \begin{vmatrix} x+iw & y+iz & 1 \\ a & i/a & 1 \\ ib & -i/b & 1 \end{vmatrix} = 0 \text{ has a solution in } \mathbb{F}_p^* \times \mathbb{F}_p^*, \tag{3.9}$$

$$c_{34}(a,b) := ab \begin{vmatrix} x+iw & y+iz & 1 \\ ia & 1/a & 1 \\ ib & -i/b & 1 \end{vmatrix} = 0 \text{ has a solution in } \mathbb{F}_p^* \times \mathbb{F}_p^*. \tag{3.10}$$

Multiplying the determinant by ab is necessary in order to get a polynomial. Note that P may lie on more than one secant. Separating the real and imaginary part of $c_{ij}(a,b)$ we obtain two equations. Taking their resultant we eliminate a and obtain a single equation in terms of b. Corresponding to each $c_{ij}(a,b)$ we obtain a polynomial $g_{ij}(b)$ by the procedure just described. We define f_{ij} in the following manner :

$$\begin{aligned} g_{ij}(x,w,y,z,b) &= \text{Resultant}(\text{Re}(c_{ij}), \text{Im}(c_{ij}), a) \\ f_{ij}(x,w,y,z,b) &= g_{ij}/(\gcd(g_{ij}, b^{\deg_b g_{ij}})). \end{aligned}$$

We do not want to consider the trivial solution $b = 0$. If x, w, y and z are such that all the polynomials $f_{ij}(b)$ have no roots in $\mathbb{F}_p^*$ then P is a missing point. This condition is a bit stronger than we need since for P to be covered both a and b must belong to $\mathbb{F}_p^*$.

3.2 Curves

Since $\mathbb{F}_{p^2} \cong \mathbb{F}_p(i) \cong \mathbb{F}_p \times \mathbb{F}_p$ we have that $AG(2,q) \cong AG(4,p)$. We would like to find curves in $AG(4,p)$ which are incident with missing points. We restrict our

attention to the following family of parameterized curves:

$$\begin{aligned} x(t) &= i_1 + i_2 t + i_3 t^2 \\ w(t) &= j_1 + j_2 t + j_3 t^2 \\ y(t) &= k_1 + k_2 t + k_3 t^2 \\ z(t) &= l_1 + l_2 t + l_3 t^2 \end{aligned}$$

where $i_1, i_2, i_3, j_1, j_2, j_3, k_1, k_2, k_3, l_1, l_2 \, and \, l_3 \in \{0, 1\}$. From now on, f_{ij} will denote the polynomial $f_{ij}(x(t), y(t), z(t), w(t)) \in \mathbb{F}_p(t)[b]$. We will focus our attention on the polynomials arising from the curve given by

$$x(t) = t^2, \, w(t) = t, \, y(t) = t^2 + t, \, z(t) = 1. \tag{3.11}$$

.

Let us consider the polynomials f_{14} and f_{23} and examine their factorizations over $\mathbb{F}_p(t, i)$. We have

$$\begin{aligned} f_{14} &= (t^2 - it + b^2(t^2 + t - i))(t^2 + it + b^2(t^2 + t + i)) \\ &\quad \times (t^2(t^2 + t)b + tb + t - b^2 - b) \\ f_{23} &= (t^2 - it + b^2(1 + i(t^2 + t)))(t^2 + it + b^2(1 - i(t^2 + t))) \\ &\quad \times (t^2 b - t(t^2 + t)b + t + (t^2 + t)b^2 - b). \end{aligned}$$

The first two factors of f_{14} are conjugates to each other. Hence a solution to the first factor is also a solution to the second factor. Consider the two curves we obtain by equating their real and imaginary parts to zero.

$$\begin{aligned} t^2 + (t^2 + t)b^2 &= 0 \\ t + b^2 &= 0 \end{aligned}$$

The only common point of intersection is $(0, 0)$. As before we do not want to

consider the trivial solution $b = 0$ and hence we ignore this point. From now on $f_{14} = t^2(t^2+t)b+tb+t-b^2-b$. Similarly, the first two factors of f_{23} are conjugates to each other. Consider the two curves obtained by equating their real and imaginary parts to zero.

$$\begin{aligned} t^2 + b^2 &= 0 \\ -t + b^2(t^2 + t) &= 0 \end{aligned}$$

The two curves intersect in at most six points by Bezout's theorem (we do not consider the $(0, 0)$ solution). Each nonzero value of t gives two points of intersection. We dismiss these three points on the curve defined by equation (3.11) corresponding to these six points of intersection. From now on $f_{23} = t^2b-t(t^2+t)b+t+(t^2+t)b^2-b$. We list on the next page the polynomials f_{ij} .

$$
\begin{aligned}
f_{11} &= b^2 + bt^3 - t \\
f_{22} &= (t+1)(b^2 + b(-t^3 - t^2 - 1)/(t+1) + 1/(t+1)) \\
f_{33} &= b^2 + b(-t^4 - t^3 - t) + t^2 \\
f_{44} &= b^2(t+1) - bt^2 + t \\
f_{12} &= (t^2 + t + 1)(b^5 + b^4(t^5 + t^3 - t - 2)/(t^2 + t + 1) + \\
&\quad b^3(-t^7 - 2t^4 - 3t^3 + 2t^2 + t + 1)/(t^2 + t + 1) \\
&\quad + b^2(2t^6 + 4t^5 + 2t^4 + 2t^3 - 2t^2)/(t^2 + t + 1) \\
&\quad + b(-t^8 - t^7 - t^6 - 2t^5 + t^4 - 2t^3)/(t^2 + t + 1) \\
&\quad + (t^5 + t^3)/(t^2 + t + 1)) \\
f_{13} &= (t^4 + 2t^3 + t^2 + 1)(b^5 + b^4(-t^8 - 3t^7 - 3t^6 - 2t^5 - 2t^4 - 2t)/(t^4 + 2t^3 + t^2 + 1) \\
&\quad + b^3(2t^6 + 2t^5 - 2t)/(t^4 + 2t^3 + t^2 + 1) + \\
&\quad b^2(t^7 + 2t^6 + 3t^3 + 2t^2 + t + 1)/(t^4 + 2t^3 + t^2 + 1) \\
&\quad + b(-2t^5 - 3t^4 - t^2 - 2t)/(t^4 + 2t^3 + t^2 + 1) \\
&\quad + (t^3 + t^2)/(t^4 + 2t^3 + t^2 + 1)) \\
f_{14} &= b^2 + b(-t^4 - t^3 - t + 1) - t \\
f_{23} &= b^2(t+1)t + b(t+1)(-t^2 + t - 1) + t \\
f_{24} &= (t^6 + 3t^5 + 3t^4 + t^3 + t^2 + t)(t^5 + 2t^4 + t^3 + t)(t^5 + 3t^4 + 3t^3 + t^2 + t + 1) \\
&\quad (b^5 + b^4(-t^6 - t^5 - t^2 + 2t - 1)/(t^5 + 2t^4 + t^3 + t) \\
&\quad + b^3(2t^6 + 4t^5 + 4t^4 + 2t^3 + 2t^2 + 2t - 2)/(t^6 + 3t^5 + 3t^4 + t^3 + t^2 + t) \\
&\quad + b^2(-t^8 - 3t^7 - 2t^6 - 2t^5 - t^4 + 3t^3 + t^2 + 4t - 1)/(t^6 + 3t^5 + 3t^4 + t^3 + t^2 + t) \\
&\quad + b(t^5 - t^4 - 3t^3 + t^2 - 2t + 2)/(t^5 + 3t^4 + 3t^3 + t^2 + t + 1) \\
&\quad + (t^2 - t)/(t^5 + 3t^4 + 3t^3 + t^2 + t + 1)) \\
f_{34} &= (t^2 + t - 1)(b^5 + b^4(-t^6 - 2t^5 + t^4 - t^2 + 2t - 2)/(t^2 + t - 1) \\
&\quad + b^3(-t^8 - t^7 - 2t^5 + t^4 + 3t^3 + t^2 + 4t - 1)/(t^2 + t - 1) \\
&\quad + b^2(-2t^6 - 4t^5 - 4t^4 - 2t^3 - 2t^2 + 2t)/(t^2 + t - 1) + \\
&\quad b(t^7 + t^5 + t^3 - t^2)/(t^2 + t - 1) + (-t^6 - t^4)/(t^2 + t - 1)).
\end{aligned}
$$

Theorem 8. *For all sufficiently large primes the polynomials f_{ij} (listed on the previous page) have the following properties.*

a. All the polynomials f_{ij} are irreducible over $\mathbb{F}_p(t)$.

b. The associated h_{20} polynomials for f_{12}, f_{13}, f_{24} and f_{34} are irreducible over $\mathbb{F}_p(t)$.

c. The square roots of the discriminants of f_{ij} do not belong to $\mathbb{F}_p(t)$.

Proof. a. The polynomials f_{ij} belong to $\mathbb{Q}[t, b]$ (clearing denominators when necessary). We look at the factorization of each f_{ij} over $\mathbb{Q}$ and find that only one of the factors involves b in each case. Further, the factor involving b is absolutely irreducible over $\mathbb{Q}$ in each case. Hence by Theorem 5 these factors are absolutely irreducible over $\mathbb{F}_p$ for sufficiently large primes. This implies f_{ij} are irreducible over $\mathbb{F}_p(t)$ for all sufficiently large primes.

b. Let $h_{20,ij}$ be the h_{20} polynomial described by Theorem 5 associated to f_{ij} for $ij \in \{12, 13, 24, 34\}$. Since the polynomials $h_{20,ij}$ belong to $\mathbb{Q}(t)[b]$ we must multiply these polynomials by suitable elements $g_{ij} \in \mathbb{Q}[t]$ to clear denominators so that $m_{ij} = h_{20,ij} g_{ij} \in \mathbb{Q}[t, b]$. We now look at the factorization of each m_{ij} over $\mathbb{Q}$ and find that only one of the factors involves b in each case. Further, the factor involving b is absolutely irreducible over $\mathbb{Q}$ in each case. Hence by Theorem 5 these factors are absolutely irreducible over $\mathbb{F}_p$ for sufficiently large primes. This implies that m_{ij} are irreducible polynomials over $\mathbb{F}_p(t)$ for sufficiently large primes. Since g_{ij} can be viewed as polynomials in $\mathbb{F}_p(t)$ (we ignore primes where $g_{ij} \equiv 0 \bmod p$) we have that $h_{20,ij}$ are irreducible polynomials over $\mathbb{F}_p(t)$ for all sufficiently large primes.

c. The discriminants of f_{ij} are not a constant times a square in $\mathbb{Q}(t)$. The third result now follows by applying Theorem 4 to the discriminants. □

3.3 Computing a Galois Group

Let F_{ij} be the splitting field of f_{ij} over $\mathbb{F}_p(t)$ and let F be the composite of these fields. Then $F/\mathbb{F}_p(t)$ is a Galois extension whose Galois group we would like to

compute. We know that $\mathcal{G}(F/\mathbb{F}_p(t))$ is the Galois Group of the splitting field of the polynomial $f(b) = \prod_{ij} f_{ij}(b)$. From Theorem 8 we have $\mathcal{G}(F_{ij}/\mathbb{F}_p(t)) \cong S_2$ for $ij \in \{11, 22, 33, 44, 14, 23\}$ and $\mathcal{G}(F_{ij}/\mathbb{F}_p(t)) \cong S_5$ for $ij \in \{12, 13, 24, 34\}$. From this information we conclude that $\mathcal{G}(F/\mathbb{F}_p(t))$ is a subgroup of $S_5^4 \times S_2^6$. In fact for the polynomials arising from equation (3.11) the Galois Group is exactly this. We make use of the following well-known theorem (see for example [5] p. 573).

Theorem 9. *Let K_1, K_2 be Galois extensions of $\mathbb{F}_p(t)$. Then*
1. The intersection $K_1 \cap K_2$ is Galois over $\mathbb{F}_p(t)$.
2. The composite K_1K_2 is Galois over $\mathbb{F}_p(t)$. The Galois Group is isomorphic to the subgroup

$$H = \{(\tau_1, \tau_2) |\, \tau_1|_{K_1 \cap K_2} = \tau_2|_{K_1 \cap K_2}\}$$

of the direct product $\mathcal{G}(K_1/\mathbb{F}_p(t)) \times \mathcal{G}(K_2/\mathbb{F}_p(t))$.

In the above theorem if $K_1 \cap K_2 = \mathbb{F}_p(t)$ then $H = \mathcal{G}(K_1/\mathbb{F}_p(t)) \times \mathcal{G}(K_2/\mathbb{F}_p(t))$.

Theorem 10. *Let $D_{ij} \in \mathbb{F}_p(t)$ be the discriminant of f_{ij} for $ij \in S = \{11, \ldots, 34\}$. Assume that the partial products*

$$\prod_{ij \in S'} D_{ij} \text{ are not squares in } \mathbb{F}_p(t) \tag{3.12}$$

where $S' \subseteq S$. Then $\mathcal{G}(F/\mathbb{F}_p(t)) = S_5^4 \times S_2^6$.

Proof. Let us begin with two extensions F_{12} and F_{13}. We know that both of them have Galois Group S_5. By Theorem 9 $F_{12} \cap F_{13}$ is a Galois extension of $\mathbb{F}_p(t)$. This implies that $\mathcal{G}(F_{12}/F_{12} \cap F_{13}) = \mathcal{G}(F_{13}/F_{12} \cap F_{13})$ are normal subgroups of S_5. Now the only non-trivial normal subgroup of S_5 is A_5. If

$$\mathcal{G}(F_{12}/F_{12} \cap F_{13}) = \mathcal{G}(F_{13}/F_{12} \cap F_{13}) = 1$$

then $F_{12} = F_{13} = F_{12} \cap F_{13}$ which contradicts condition (3.12). If

$$\mathcal{G}(F_{12}/F_{12} \cap F_{13}) = \mathcal{G}(F_{13}/F_{12} \cap F_{13}) = A_5$$

then $\mathcal{G}(F_{12} \cap F_{13}/\mathbb{F}_p(t))$ is a degree two extension. This implies that

$$F_{12} \cap F_{13} = \mathbb{F}_p(t, \sqrt{D_{12}}) = \mathbb{F}_p(t, \sqrt{D_{13}}).$$

This is a contradiction to condition (3.12). Therefore we conclude that

$$\mathcal{G}(F_{12}/F_{12} \cap F_{13}) = \mathcal{G}(F_{13}/F_{12} \cap F_{13}) = S_5.$$

This implies $F_{12} \cap F_{13} = \mathbb{F}_p(t)$. By Theorem 9 we have $\mathcal{G}(F_{12}F_{13}/\mathbb{F}_p(t)) = S_5 \times S_5$.

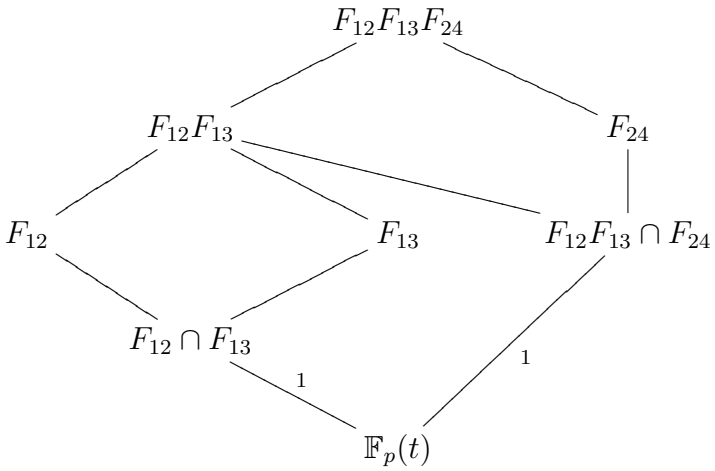

Figure 3.1: Hasse Diagram for Theorem 10

We now apply Theorem 9 to the Galois extensions $F_{12}F_{13}$ and F_{24}.We will prove that $F_{12}F_{13} \cap F_{24} = F_p(t)$. By Theorem 9 the extension is Galois.This implies $\mathcal{G}(F_{24}/F_{12}F_{13} \cap F_{24})$ is a normal subgroup of S_5. If

$$\mathcal{G}(F_{24}/F_{12}F_{13} \cap F_{24}) = 1$$

then $F_{12} = F_{13} = F_{24}$ contradicting condition (3.12). If

$$\mathcal{G}(F_{24}/F_{12}F_{13} \cap F_{24}) = A_5$$

then $F_{12}F_{13} \cap F_{24}/\mathbb{F}_p(t)$ is a degree two extension. This implies

$$F_{12}F_{13} \cap F_{24} = \mathbb{F}_p(t, \sqrt{D_{24}}).$$

We know that the only degree two subfields of $F_{12}F_{13}$ are $\mathbb{F}_p(t, \sqrt{D_{12}})$, $\mathbb{F}_p(t, \sqrt{D_{13}})$ and $\mathbb{F}_p(t, \sqrt{D_{12}D_{13}})$. If

$$F_{12}F_{13} \cap F_{24} = \mathbb{F}_p(t, \sqrt{D_{24}})$$

is equal to any of these then condition (3.12) is violated. Hence $\mathcal{G}(F_{24}/F_{12}F_{13} \cap F_{24}) = S_5$ and this implies $F_{12}F_{13} \cap F_{24} = \mathbb{F}_p(t)$. Therefore

$$\mathcal{G}(F_{12}F_{13}F_{24}/\mathbb{F}_p(t)) = S_5 \times S_5 \times S_5.$$

We apply Theorem 9 now to the fields $F_{12}F_{13}F_{24}$ and F_{34}. A similar argument leads us to conclude that $\mathcal{G}(F_{12}F_{13}F_{24}F_{34}/\mathbb{F}_p(t)) = S_5 \times S_5 \times S_5 \times S_5$.

Next, we deal with the degree 2 extensions. We know

$$F_{ij} = \mathbb{F}_p(t, \sqrt{D_{ij}})$$

for $ij \in \{11, 22, 33, 44, 14, 23\}$. Let us apply Theorem 9 to $F_{12}F_{13}F_{24}F_{34}$ and F_{11}. Clearly $F_{12}F_{13}F_{24}F_{34} \cap F_{11}$ is a field of degree at most 2 over $\mathbb{F}_p(t)$. If the degree is 2 then $F_{11} \subseteq F_{12}F_{13}F_{24}F_{34}$. But this would again violate condition (3.12). Hence $F_{12}F_{13}F_{24}F_{34} \cap F_{11} = \mathbb{F}_p(t)$. Therefore

$$\mathcal{G}(F_{12}F_{13}F_{24}F_{11}/\mathbb{F}_p(t)) = S_5^4 \times S_2.$$

Proceeding in this manner we prove that $\mathcal{G}(F/\mathbb{F}_p(t)) = S_5^4 \times S_2^6$.

□

We have the following theorem.

Theorem 11. *For all sufficiently large primes the following result is true for the polynomials f_{ij} arising from the curve described by equation (3.11):*

$$\prod_{ij \in S'} D_{ij} \text{ is not a square of a polynomial in } \mathbb{F}_p(t), \tag{3.13}$$

where $S' \subseteq S = \{11, \ldots, 34\}$. Further, none of the partial products are a constant times a square.

Proof. Since none of the partial products are a constant times a square in $\mathbb{Q}(t)$ the result follows by applying Theorem 4 to the partial products. □

3.4 Applying the Čebotarev Density Theorem

To apply the density theorem we want to show that the algebraic closure of $\mathbb{F}_p$ in F is the finite field itself. Let $L = \mathbb{F}_{p^n}$ be the algebraic closure of $\mathbb{F}_p$ in F. By Theorem 11,

$$[\mathbb{F}_{p^n}(t, \sqrt{D_{11}}, \ldots, \sqrt{D_{34}}) : \mathbb{F}_p(t, \sqrt{D_{11}}, \ldots, \sqrt{D_{34}})] = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n.$$

We know that $\mathcal{G}(F/\mathbb{F}_p(t, \sqrt{D_{11}}, \ldots, \sqrt{D_{34}})) \cong A_5^4$. Now

$$\mathbb{F}_{p^n}(t, \sqrt{D_{11}}, \ldots, \sqrt{D_{34}})/\mathbb{F}_p(t, \sqrt{D_{11}}, \ldots, \sqrt{D_{34}})$$

is a Galois extension with a cyclic Galois group.

Therefore we conclude $\mathcal{G}(F/\mathbb{F}_{p^n}(t, \sqrt{D_{11}}, \ldots, \sqrt{D_{34}}))$ is a normal subgroup of A_5^4 whose quotient group is cyclic. But no such non-trivial normal subgroup of A_5^4 exists. Hence n must be one i.e. $\mathbb{F}_p$ is algebraically closed in F and we can apply Theorem 6.

Let $t_0 \in \mathbb{F}_p$. If we apply Theorem 6 to the Galois extensions arising from polynomials of degree 2 (such as f_{11}) and degree 5 (such as f_{12}) which satisfy the hypothesis of the theorem.

Representative of the Conjugacy Class	No. of roots in $\mathbb{F}_p$	Number of elements in the
1	$f_{11}(t_0, b)$ has 2 roots in $\mathbb{F}_p$	$\frac{1}{2}p + O(\sqrt{p})$
(12)	$f_{11}(t_0, b)$ has no roots in $\mathbb{F}_p$	$\frac{1}{2}p + O(\sqrt{p})$

Representative of the Conjugacy Class	No. of roots in $\mathbb{F}_p$	Number of elements
1	$f_{12}(t_0, b)$ has 5 roots in $\mathbb{F}_p$	$\frac{1}{120}p + O(\sqrt{p})$
(12)	$f_{12}(t_0, b)$ has 3 roots in $\mathbb{F}_p$	$\frac{1}{12}p + O(\sqrt{p})$
(123)	$f_{12}(t_0, b)$ has 2 roots in $\mathbb{F}_p$	$\frac{1}{6}p + O(\sqrt{p})$
(1234)	$f_{12}(t_0, b)$ has 1 root in $\mathbb{F}_p$	$\frac{1}{4}p + O(\sqrt{p})$
(12345)	$f_{12}(t_0, b)$ has no roots in $\mathbb{F}_p$	$\frac{1}{5}p + O(\sqrt{p})$
(12)(34)	$f_{12}(t_0, b)$ has 1 root in $\mathbb{F}_p$	$\frac{1}{8}p + O(\sqrt{p})$
(12)(345)	$f_{12}(t_0, b)$ has no roots in $\mathbb{F}_p$	$\frac{1}{6}p + O(\sqrt{p})$

Let us now apply Theorem 6 to the Galois extension $F/\mathbb{F}_p(t)$. We have just computed the Galois Group of $F/\mathbb{F}_p(t)$. We want to find the number of $t_0 \in \mathbb{F}_p$ such that $f(t_0, b)$ has no solutions in $\mathbb{F}_p^*$. The Conjugacy classes of $\mathcal{G}(F/\mathbb{F}_p(t))$ are nothing but the direct product of the Conjugacy classes of $\mathcal{G}(F_{ij}/\mathbb{F}_p(t))$. The representatives of the Conjugacy classes corresponding to which $f(t_0, b)$ has no solution in $\mathbb{F}_p$ are $(12)^6 \times ((12345))^{n_1} \times ((12)(345))^{n_2}$ where $n_1 + n_2 = 4$. Hence the cardinality of the set $\{t \in \mathbb{F}_p | f(t, b)$ has no solution in $\mathbb{F}_p^*\}$ is $(\frac{1}{2})^6(\frac{1}{5} + \frac{1}{6})^4 p + O(\sqrt{p})$.

We have just proved that for all sufficiently large primes the approximate number of the points on the curve described by equation (3.11) which are not covered by the arc K is $\frac{14641}{51840000}p$. This is exactly what Theorem 2 states. Hence the arc K is never complete for all sufficiently large primes.

Chapter 4

Extending the Giulietti-Ughi arc

4.1 Adding points

The natural question which arises is how many of these points on the curve given by (3.11) may be added to K to form a larger arc. We know that $P(t) = (t^2+it, t^2+t+i)$ for $t \in \mathbb{F}_p$ is a point on the curve defined by equation (3.11). We define

$$T := \{t \in \mathbb{F}_p \mid K \cup P(t) \text{ is a arc}\}$$

and

$$R := \{s \in T \mid K \cup \{P(s), P(t)\} \text{is an arc} \, \forall \, t \in T\}.$$

We also define $P(R) := \{P(s) \mid s \in R\}$.

Theorem 12. *$K \cup P(R)$ is an arc.*

Proof. There are three types of secants formed by joining two points in $K \cup P(R)$.
a) Secants formed by joining two points in K.
b) Secants formed by joining one point in K and another in $P(R)$.
c) Secants formed by joining two points in $P(R)$.
If we prove that none of the secants intersect $K \cup P(R)$ in a third point then the set is an arc. A secant of type a) cannot be incident with a third point in K since K is an arc. It also cannot be incident with a point in $P(R)$ since $P(R)$ consists of only missing points of K. A secant of type b) cannot be incident with a third

point in K because every point in $P(R)$ is a missing point of K. It also cannot be incident with a third point of $P(R)$ since that would contradict the property of the set $P(R)$. A secant of type c) cannot be incident with a point in K because it would then be a secant of type b) and we have just shown that a secant of type b) is not incident with three points of the set $K \cup P(R)$. Finally a secant of type c) cannot be incident with a third point of $P(R)$ because any line meets the curve described by equation (3.11) in at most two points.

□

4.2 Conditions for a point on the curve to be a missing point

We now prove that the set R is not empty. The condition that a point $P(s)$ is covered by a line formed by joining a point in K_1 and a point in T is

$$c_1(a,t) := a \begin{vmatrix} s^2+is & s^2+s+i & 1 \\ t^2+it & t^2+t+i & 1 \\ a & 1/a & 1 \end{vmatrix} = 0 \text{ has a solution in } \mathbb{F}_p^* \times T. \tag{4.1}$$

Similarly conditions for a point $P(s)$ to be covered by a line formed by joining a point in K_i $(i = 2, 3, 4)$ and a point in T are:

$$c_2(a,t) := a \begin{vmatrix} s^2+is & s^2+s+i & 1 \\ t^2+it & t^2+t+i & 1 \\ ia & 1/a & 1 \end{vmatrix} = 0 \text{ has a solution in } \mathbb{F}_p^* \times T, \tag{4.2}$$

$$c_3(a,t) := a \begin{vmatrix} s^2+is & s^2+s+i & 1 \\ t^2+it & t^2+t+i & 1 \\ a & i/a & 1 \end{vmatrix} = 0 \text{ has a solution in } \mathbb{F}_p^* \times T, \tag{4.3}$$

$$c_4(a,t) := a\begin{vmatrix} s^2+is & s^2+s+i & 1 \\ t^2+it & t^2+t+i & 1 \\ ia & -i/a & 1 \end{vmatrix} = 0 \text{ has a solution in } \mathbb{F}_p^* \times T \qquad (4.4)$$

respectively. Multiplying the polynomial by a is necessary in order to get a polynomial. We define the following equations.

$$\begin{aligned} \hat{c}_j(t,s) &= \text{Resultant}(\text{Re}(c_j(t,s,a)), \text{Im}(c_j(t,s,a)), a) \\ f_j(t,s) &= \hat{c}_j/(\gcd(\hat{c}_j, (t-s)^{(\deg(\hat{c}_j))})) \end{aligned}$$

for $j = 1, 2, 3, 4$. We prove the following result about these polynomials.

Theorem 13. *For all sufficiently large primes the polynomials f_j, where $j \in U = \{1,2,3,4\}$, have the following properties.*
a. f_j is an irreducible polynomial of degree 3 over $\mathbb{F}_p(t)$.
b. Let $D_j \in \mathbb{F}_p(t)$ be the discriminant of f_j; then, $\sqrt{D_j}$ is not in $\mathbb{F}_p(t)$.

Proof. a. The polynomials f_j belong to $\mathbb{Q}[t,s]$ and are absolutely irreducible over $\mathbb{Q}$. Hence by Theorem 5 these polynomials are absolutely irreducible over $\mathbb{F}_p$ for sufficiently large primes. This implies f_j are irreducible over $\mathbb{F}_p(t)$ for sufficiently large primes.

b. The discriminants D_j associated to f_1, f_2, f_3 and f_4 are not a constant times a square in $\mathbb{Q}(t)$. The second result now follows by applying Theorem 4 to the discriminants.. □

Let F_j be the splitting field of f_j over $\mathbb{F}_p(t)$ and let $E = FF_1F_2F_3F_4$. Then $E/\mathbb{F}_p(t)$ is a Galois extension whose Galois group we would like to compute. We know that $\mathcal{G}(E/\mathbb{F}_p(t))$ is the Galois Group of the splitting field of the polynomial

$$e(t,s) = \prod_{ij} f_{ij}(t,s) \prod_j f_j(t,s)$$

when considered as a univariate polynomial defined over $\mathbb{F}_p(t)$. From Theorem 12 we have $\mathcal{G}(F_j/\mathbb{F}_p(t)) \cong S_3$ for $j \in \{1,2,3,4\}$ and $\mathcal{G}(F/\mathbb{F}_p(t)) \cong S_5^4 \times S_2^6$. From this information we conclude that $\mathcal{G}(E/\mathbb{F}_p(t))$ is a subgroup of $S_5^4 \times S_2^6 \times S_3^4$. In fact for

the polynomials arising from the curve defined by equation (3.11) the Galois Group is exactly this.

Theorem 14. *For all sufficiently large primes the polynomials f_j, with $j \in U = \{1, 2, 3, 4\}$, have the following properties.*

$$\prod_{ij \in S'} D_{ij} \prod_{j \in U'} D_j \text{ is not a square in } F_p(t), \tag{4.5}$$

where $S' \subseteq S$ and $U' \subseteq U$. Further, none of the partial products are a constant times a square.

Proof. Since none of the partial products are a constant times a square in $\mathbb{Q}(t)$ the result follows by applying Theorem 4 to the partial products. □

4.3 Computing another Galois Group

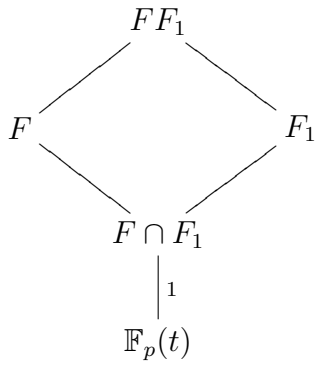

Figure 4.1: Hasse Diagram for FF_1

By Theorem 9 we have that $F \cap F_1$ is a Galois extension of $\mathbb{F}_p(t)$.This implies $\mathcal{G}(F_1/F \cap F_1)$ is a normal subgroup of S_3. The only non-trivial normal subgroup of S_3 is A_3. If

$$\mathcal{G}(F_1/F \cap F_1) = 1$$

then $F \subseteq F_1$ which contradicts condition (4.18). If

$$\mathcal{G}(F_1/F \cap F_1) = A_3$$

then $\mathbb{F}_p(t, \sqrt{D_1}) \subset F$. This again is a contradiction to condition (4.18). Hence $\mathcal{G}(F_1/F \cap F_1) = S_3$ which implies $F \cap F_1 = \mathbb{F}_p(t)$. By Theorem 9 we have

$$\mathcal{G}(FF_1/\mathbb{F}_p(t)) = \mathcal{G}(F/\mathbb{F}_p(t)) \times S_3.$$

Similarly applying Theorem 9 to FF_1 and F_2 we have

$$\mathcal{G}(FF_1F_2/\mathbb{F}_p(t)) = \mathcal{G}(F/\mathbb{F}_p(t)) \times S_3^2.$$

Proceeding in this manner we conclude that $\mathcal{G}(E/\mathbb{F}_p(t)) = S_5^4 \times S_2^6 \times S_3^4$.

4.4 Applying the Čebotarev Density Theorem

To apply the density theorem to the extension $E/\mathbb{F}_p(t)$ we have to show that $\mathbb{F}_p$ to be algebraically closed in E. Let $H = \mathbb{F}_{p^m}$ be the algebraic closure of $\mathbb{F}_p$ in E. By Theorem 13,

$$[\mathbb{F}_{p^m}(t, \sqrt{D_{11}}, \ldots, \sqrt{D_4}) : \mathbb{F}_p(t, \sqrt{D_{11}}, \ldots, \sqrt{D_4})] = [\mathbb{F}_{p^m} : \mathbb{F}_p] = m$$

. We know that $\mathcal{G}(F/\mathbb{F}_p(t, \sqrt{D_{11}}, \ldots, \sqrt{D_4})) = A_5^4 \times A_3^4$. Now

$$\mathbb{F}_{p^m}(t, \sqrt{D_{11}}, \ldots, \sqrt{D_{34}})/\mathbb{F}_p(t, \sqrt{D_{11}}, \ldots, \sqrt{D_4})$$

is a Galois extension with a cyclic Galois group. Hence

$$\mathcal{G}(F/\mathbb{F}_{p^m}(t, \sqrt{D_{11}}, \ldots, \sqrt{D_4}))$$

is a normal subgroup of $A_5^4 \times A_3^4$ whose corresponding quotient group

$$M = \mathcal{G}(\mathbb{F}_{p^m}(t, \sqrt{D_{11}}, \ldots, \sqrt{D_1})/\mathbb{F}_p(t, \sqrt{D_{11}}, \ldots, \sqrt{D_1}))$$

is cyclic. The only two possible choices for M are 1 and A_3. If $M = A_3$ then $m = 3$. Since $\mathbb{F}_{p^m}(t)/\mathbb{F}_p(t)$ is a Galois extension it follows that $\mathcal{G}(E/\mathbb{F}_{p^m}(t))$ is an index three normal subgroup of $S_5^4 \times S_2^6 \times S_3^4$. But no such subgroup exists and hence

$M = 1$. This implies that $m = 1$ i.e. $\mathbb{F}_p$ is algebraically closed in E.

Let $t_0 \in \mathbb{F}_p$. If we apply Theorem 6 to the Galois extensions arising from polynomials of degree 3 (such as f_1) which satisfy the hypothesis of the theorem.

Representative of the Conjugacy Class	No. of roots in $\mathbb{F}_p$	Number of elements
1	$f_1(t_0, s)$ has 3 roots in $\mathbb{F}_p$	$\frac{1}{6}p + O(\sqrt{p})$
(12)	$f_1(t_0, s)$ has 1 root in $\mathbb{F}_p$	$\frac{1}{2}p + O(\sqrt{p})$
(123)	$f_1(t_0, s)$ has no roots in $\mathbb{F}_p$	$\frac{1}{3}p + O(\sqrt{p})$

The Conjugacy classes of $\mathcal{G}(E/\mathbb{F}_p(t))$ are direct product of the Conjugacy classes of $\mathcal{G}(F_{ij}/\mathbb{F}_p(t))$ and $\mathcal{G}(F_i/\mathbb{F}_p(t))$. The representatives of the Conjugacy classes corresponding to which $e(t_0, s)$ has no solution in $\mathbb{F}_p$ are $(12)^6 \times ((12345))^{n_1} \times ((12)(345))^{n_2} \times (123)^4$ where $n_1 + n_2 = 4$. The set R can alternatively be described as the set $\{t \in \mathbb{F}_p | e(t, s) \text{ has no solution in } \mathbb{F}_p\}$. The cardinality of this set by the Density theorem is $(\frac{1}{2})^6(\frac{11}{30})^4(\frac{1}{3})^4 p + O(\sqrt{p})$. This is what Theorem 3 states.

Chapter 5

What Next ?

From the first chapter we know that the size of the smallest complete arc in $PG(2, q)$ satisfies

$$\sqrt{2q} \leq n_q \leq \sqrt{q} \log^c q \tag{5.1}$$

where c is some universal constant. However, a complete arc with cardinality in this interval has not been explicitly constructed. The arc constructed by Giulietti and Ughi is close to the lower bound for all primes $p \equiv 3 \bmod 4$ and $p \leq 31$ and is complete. However it fails to be complete for larger primes.

The natural question one could ask is that is it possible to add more points to the original construction in order to obtain a small complete arc for all primes. For large primes the curve described by equation (3.11) has certain "nice" properties but is by no means unique. This leads us to conjecture that we should be able to add more points on curves of degree 2 to the original construction of Giulietti and Ughi to obtain a complete arc of small cardinality.

We know from Theorem 4 that the number of missing points on the curve given by equation (3.11) is some proportion of p . Based on this observation we propose the following construction. At each step we should consider a curve of degree 2 and add points on this curve to our arc to obtain a larger arc. At the i^{th} step we choose the curve C_i and add $c_i(p)\sqrt{q}$ points. As we keeping adding more points to our arc the number of missing points should become smaller and hopefully $c_i(p) \geq c_j(p)$ for $i < j$. For each prime we expect the process to terminate after a finite number of

steps and eventually we hope to construct a complete arc. This complete arc should have

$$\sum_{i=1}^{m_q} c_i(p)\sqrt{q}$$

points where m_q is the number of curves we have to add in order to obtain a complete arc. Fisher conjectured that the average size of a complete arc is $\sqrt{3q\log q}$ ([6]). Keeping this in mind we conjecture that

$$\sum c(p) < O(\log q).$$

We expect the number of points in this complete arc to have cardinality $O(\sqrt{q}\log q)$ and depending on c this number should be close to the upper bound of inequality (5.1).

Bibliography

[1] S. Ball. On small complete arcs in a finite plane. *Discrete Math.*, 174(1-3):29–34, 1997. Combinatorics (Rome and Montesilvano, 1994).

[2] A. Blokhuis. Polynomials in finite geometries and combinatorics. In *Surveys in combinatorics, 1993 (Keele)*, volume 187 of *London Math. Soc. Lecture Note Ser.*, pages 35–52. Cambridge Univ. Press, Cambridge, 1993.

[3] A. Blokhuis. Extremal problems in finite geometries. In *Extremal problems for finite sets (Visegrád, 1991)*, volume 3 of *Bolyai Soc. Math. Stud.*, pages 111–135. János Bolyai Math. Soc., Budapest, 1994.

[4] D. S. Dummit. Solving solvable quintics. *Math. Comp.*, 57(195):387–401, 1991.

[5] D. S. Dummit and R. M. Foote. *Abstract algebra*. Prentice Hall Inc., Englewood Cliffs, NJ, 1991.

[6] J.C. Fisher. Random k-arcs. *Preliminary Report*, 1989.

[7] M. D. Fried and M. Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 2005.

[8] M. Giulietti and E. Ughi. A small complete arc in $\mathrm{PG}(2, q)$, $q = p^2$, $p \equiv 3 \pmod 4$. *Discrete Math.*, 208/209:311–318, 1999. Combinatorics (Assisi, 1996).

[9] J. W. P. Hirschfeld. Maximum sets in finite projective spaces. In *Surveys in combinatorics (Southampton, 1983)*, volume 82 of *London Math. Soc. Lecture Note Ser.*, pages 55–76. Cambridge Univ. Press, Cambridge, 1983.

[10] J. W. P. Hirschfeld. *Projective geometries over finite fields*. The Clarendon Press Oxford University Press, New York, 1988. Oxford Mathematical Monographs.

[11] J. H. Kim and V. H. Vu. Small complete arcs in projective planes. *Combinatorica*, 23(2):311–363, 2003.

[12] G. Shimura. Reduction of algebraic varieties with respect to a discrete valuation of the basic field. *Amer. J. Math.*, 77:134–176, 1955.

[13] T. Szőnyi. Some applications of algebraic curves in finite geometry and combinatorics. In *Surveys in combinatorics, 1997 (London)*, volume 241 of *London Math. Soc. Lecture Note Ser.*, pages 197–236. Cambridge Univ. Press, Cambridge, 1997.

[14] J. F. Voloch. Arcs in projective planes over prime fields. *J. Geom.*, 38(1-2):198–200, 1990.

[15] J. F. Voloch. Complete arcs in Galois planes of nonsquare order. In *Advances in finite geometries and designs (Chelwood Gate, 1990)*, Oxford Sci. Publ., pages 401–406. Oxford Univ. Press, New York, 1991.

VITA

Rohit Ghosh was born in Mumbai, India on February 11, 1978. Growing up in Kolkatta, India, he attended high school at Calcutta Boys School. In 1995, he graduated and entered Saint Xavier's College Kolkatta, India. He received a Bachelor of Science degree in Mathematics in May 1998 and then obtained a Masters degree from the Ramanujan Institute in December 1999. After spending eight months at Texas A & M university he began work on a Doctorate of Philosophy in the Mathematics Department of the University of Texas, Austin in September 2001 .

Permanent Address: 921 E 46th St 207 Austin, Tx-78751

This dissertation was typed by the author.